PC 530.5:

Unauthorized Use of Personal Identifying Information

a) Every person who willfully obtains personal identifying information, as defined in subdivision (b), of another person without the authorization of that person, and uses that information in the name of the other person without the consent of that person is guilty of a public offense.

What is Identity Theft?

Identity theft involves acquiring key pieces of someone's identifying information such as name, address, date of birth, social security number and mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud which include, but are not limited to, taking over the victim's financial accounts, opening new bank accounts, purchasing automobiles, applying for loans, credit cards and social security benefits, renting apartments, and establishing services with utility and phone companies.

What to do if you become a victim:

- Set up a folder to keep a detailed history of this crime.
- Keep a log of all your contacts and make copies of all documents.
- Contact all creditors, by phone and in writing to inform them of the problem.
- Notify the US Postal Inspector if your mail has been stolen or tampered with:
 - US Postal Inspectors Service (See phone listing under Federal Government.)
 - US Postal Inspector Service- Local Post Office (See phone listing under Federal Government.)

www.usps.gov/websites/depart/inspect

- Contact the Federal Trade Commission to report the problem:
 - <u>www/ftc.gov</u> The FTC is the federal dearinghouse for complaints by victims of identity theft. The FTC helps victims by providing information to help resolve financial and other problems that could result in identity theft. Their hotline telephone number is 1-877-IDTHEFT (438-4338.)

Sample "Courtesy Notice"

(Date)

Dear (Creditor Name/Collection Agency Name:)

On (date), I received your letter demanding payment of (\$ amount). I did not open this account and incur this unpaid balance. Someone, other than myself, wrongfully used my personal information to obtain a line of credit/service. Your company extended a line of credit/services to someone, other than myself. Your company is a victim and should file a police report in the appropriate jurisdiction.

You are hereby notified that on (date), I filed an identity theft report with the Placer County Sheriff's Department. The case number is (_______), a copy of which can be obtained by contacting PCSO records division at (530) 889-7800.

(Your name and address)

• Call each of the three credit bureaus' fraud units to report identity theft. Ask to have a "Fraud Alert/Victim Impact" statement placed in your credit file asking that creditors call you before opening any new accounts.

Request that a copy of your credit report be sent to you.

CREDIT BUREAUS

Equifax

P.O. Box 74021, Atlanta, Georgia 30374-0241

- To order your report, call 1-800-685-1111
- To report fraud, call 1-800-525-6285

Experian

P.O. Box 949, Allen, Texas 75013-0949

- To order your report, call 1-888-397-3742
- To report fraud, call 1-888-397-3742

Trans Union

P.O. Box 390, Springfield, Pennsylvania 19064-0390

- To order your report, call 1-800-916-8800
- To report fraud, call 1-800-680-7289

Alert your banks to flag your accounts and contact you to confirm any unusual activity. Request a change of PIN and a new password.

If you have any checks stolen or bank accounts set up fraudulently, report it to the following companies:

National Check Fraud Service- (843) 571-2143 SCAN- (800) 262-7771 TeleCheck- (800) 710-9898 or 927-0188 CheckRite- (800) 766-2748 Equifax Check Systems- (800) 437-5120 International Check Service- (800) 526-5380

- Contact the Social Security Administration's Fraud Hotline at 1-800-269-0271/
- Contact the state office of the Department of Motor Vehicles to see if another license was issued in your name. If so, request a new license number and fill out the DMV's complaint form to begin the fraud investigation process.
- Obtain description of suspect (if known.)
- Obtain witness information.
- What is the financial loss to you? Attach all supporting documentation.

Preventive Actions

- Promptly remove mail from your mailbox after delivery.
- Deposit outgoing mail in post office collection mailboxes at your local post office. Do not leave in unsecured mail receptacles.
- Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, or bank PIN code, unless you initiated the call. Protect this information and release it only when absolutely necessary.
- Shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want before discarding them in the trash or recycling bin.
- Empty your wallet of extra credit cards and ID's, or better yet, cancel the ones you do not use and maintain a list of the ones you do.
- Order your credit report from the three credit bureaus once a year to check for fraudulent activity or other discrepancies.
- Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gasoline pumps. Keep track of all your paperwork. When you no longer need it, destroy it.
- Memorize your social security number and all of your passwords. Do not record them on any cards or on anything in your wallet or purse.

- Sign all new credit cards upon receipt.
- Save all credit card receipts and match them against your monthly bills.
- Be conscious of normal receipt of routine financial statements. Contact the sender of they are not received in the mail.
- Notify your credit card companies and financial institution in advance of any change of address or phone number.
- Never loan your credit cards to anyone else.
- Never put your credit card or any other financial account number on a postcard or on the outside of an envelope.
- If you applied for a new credit card and it hasn't arrived in a timely manner, call the bank or credit card company involved.
- Report all lost or stolen credit cards immediately.
- Closely monitor expiration dates on your credit cards. Contact the credit card issuer if replacement cards are not received prior to the expiration date.
- Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.

Internet and On-Line Services

- Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any Web site or on-line service location unless you receive a secured authentication key from your provider.
- When you subscribe to an on-line service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number used to subscribe. Don't give them out?

Victim's Rights to Fraudulent Application Information 530.8 PC

A person who discovers that an unauthorized application in his or her name has been made for a loan, credit line or account, credit card, charge card, or utility service, or that an unauthorized account in his or her name has been opened with a bank, trust company, savings association, credit union, or utility, is, upon presentation of a copy of the police report, entitled to receive from the entity to which the unauthorized application or account was made, a copy of the unauthorized application or account information for, and a record of, transactions or charges associated with the unauthorized application or account. Upon request, the entity receiving the application or opening the account shall inform the victim what false information the suspect used in making the unauthorized application or account.

Your	PCSO	Case Number	is	

Make note of this case number in your detailed history folder and reference it when you have contact with any business or law enforcement agency concerning this report. Depending upon the location (jurisdiction) of where the crime occurred (goods or services obtained or delivered,) an investigator may or may not be assigned to this case.

If the crime occurred in our jurisdiction and there are workable leads, such as witnesses and suspect information, an investigator will be assigned to the case. Unfortunately, not all cases will be assigned to an investigator because there are no significant leads to identify the suspect.

INFORMATIONAL WEB SITES

Federal Trade Commission www.ftc.gov

California Department of Consumer Affairs <u>www.dcs.ca.gov</u>

Privacy Rights Clearing House www.privacyrights.org

U.S. Government Accounting Office www.gao.gov

U.S. Postal Inspection Service www.usps.gov/postalinspectors

International Association of Financial Crimes Investigators <u>www.jafci.org</u> (go to links section)

> Placer County Sheriff's Department 11500 A Ave. Auburn, CA 95604

> > (530) 889-7800 www.placer.ca.gov/sheriff